Euler's Generalization of Fermat's thm

Euler's phi-function $n \geq 1$, $\phi(n)$ = No. of positive integers not exceeding n that are relatively prime to n.

[or Totient / Totient]

Example 1) $n = 20$ $\quad \phi(20) = 8 = \{1, 3, 7, 9, 11, 13, 17, 19\}$

2) If $n = p \leftarrow$ prime then $\phi(p) = p - 1$

If $p = 5$ $\quad \gcd(1,5) = \gcd(2,5) = \gcd(3,5) = \gcd(4,5) = 1$

$\therefore \phi(5) = 4 = 5 - 1$

Thm: If p is a prime and $k > 0$ then

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

Pf The integers between 1 and p^k that are divisible by p are

$$p, 2p, \ldots (p^{k-1})p$$

This list contains p^{k-1} integers

$\therefore$ The no. of integers between 1 and p^k that are relatively prime to p^k are $= p^k - p^{k-1}$ i.e.

$$\phi(p^k) = p^k - p^{k-1}$$

$$= p^k\left(1 - \frac{1}{p}\right)$$

Example Find $\phi(27)$

Sol $27 = 3^3$

$$\therefore \phi(27) = 3^3\left(1 - \frac{1}{3}\right) = 3^3 \cdot \frac{2}{3} = 18.$$

Lemma Let $a, b, c \in \mathbb{Z}$. Then $\gcd(a, bc) = 1$ iff $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$

Pf Suppose $\gcd(a, bc) = 1$

Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$

$\Rightarrow d \mid a$ and $d \mid bc$

$\Rightarrow \gcd(a, bc) \geq d$

$\Rightarrow 1 \geq d \Rightarrow d = 1$

Similarly we can prove that $\gcd(a, c) = 1$

Conversely suppose $\gcd(a, b) = 1 = \gcd(a, c)$

Let us assume that $\gcd(a, bc) = d_1 > 1$

Hence $\exists$ p prime s.t. $p \mid d_1$

$\Rightarrow p \mid a$ and $p \mid bc$

$\Rightarrow$ " and $p \mid b$ OR $p \mid c$

$\Rightarrow \gcd(a, b) \geq p$ ~~$\leftarrow$ contradiction~~ OR $\gcd(a, c) \geq$

This is a contradiction

Hence $d_1 = 1$ i.e. $\gcd(a, bc) = 1$

Thm The function ϕ is a multiplicative function.

Pf Let $m, n \in \mathbb{N}$ s.t. $\gcd(m,n)=1$

To show $\phi(mn)=\phi(m)\phi(n)$

Case I If $m=1$ or $n=1$ the result easily follows

Case II Both $m>1$ and $n>1$

Arrange the integers from 1 to mn in the following way

1	2	... (r) ...	m
$m+1$	$m+2$	$m+r$	$2m$
$2m+1$	$2m+2$	$2m+r$	$3m$
⋮	⋮	⋮	⋮
$(n-1)m+1$	$(n-1)m+2$	$(n-1)m+r$	nm

We know that $\phi(mn)$ is equal to the number of entries in this array that are relatively prime to mn.

Now we know that an integer is relatively prime to mn iff it is relatively prime to both m and n (See previous lemma)

By Euclid's algorithm to find GCD we know that

$\gcd(qm+r, m) = \gcd(r, m)$

($qm+r$: No. in the rth column; r: No. in 1st row and rth column)

$\therefore \gcd(qm+r, m) = \gcd(r, m)$

$\therefore$ Nos in the rth column are relatively prime to m iff $\gcd(r,m)=1$ i.e. r itself is relatively prime to m.

$\therefore$ No. of columns containing integers prime to m is precisely the no of integers less than m and relatively prime to m i.e. $\phi(m)$.

Now in each column we will count the number of integers that are relatively prime to n.

The resulting integers will be relatively prime to both

m and ~~km~~ n and hence will be relatively prime to mn.

The entries in the r^{th} column are given by (r s.t $\gcd(r, m) = 1$)

$$\underbrace{r, mn+r, 2mn+r, \ldots, (n-1)m+r}_{n \text{ integers}}$$

Claim: $km + r \not\equiv jm + r \pmod{m}$ $\quad 0 \le k, j \le n-1 < n$

Proof: Suppose $km + r \equiv jm + r \pmod{m}$ $\quad 0 \le k, j \le n-1 < n$

$\Rightarrow km \equiv jm \pmod{m}$

$\Rightarrow k \equiv j \pmod{m}$ $\quad [\because \gcd(m, m) = 1]$

$\Rightarrow n \mid k - j$ $\quad \leftarrow$ Impossible

~~The~~ We know that if n divides any of these listed integers the possible remainders are

$$\underbrace{0, 1, 2, 3, \ldots, n-1}_{n \text{ integers}}$$

and by the claim (that we just proved) we get ~~unto~~ n unique congruences of the following type:

$$km + r \equiv j \pmod{m} \qquad 0 \le k, j \le n-1$$

$$\Rightarrow \gcd(km + r, m) = \gcd(j, m)$$

Hence $\gcd(km + r, m) = 1$ iff $\gcd(j, m) = 1$

$\therefore$ No. of integers in the r^{th} column that are relative prime to m is $\phi(m)$.

$\therefore$ Total no. of integers relatively prime to mn is $\phi(m)\phi(n)$

Hence $\phi(mn) = \phi(m)\phi(n)$

Thm 3 If $n \in \mathbb{N}$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ then

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_s^{k_s} - p_s^{k_s-1})$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right)$$

Pf We will use induction on n.

The result is true for $n = 1$ by Thm 1.

Suppose the result is true for $n = i$.

$\because$ $\gcd(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}, p_{i+1}^{k_{i+1}}) = 1$

$\therefore$ $\phi\left((p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}) p_{i+1}^{k_{i+1}}\right) = \phi(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i})\,\phi(p_{i+1}^{k_{i+1}})$

$$= \left[(p_1^{k_1} - p_1^{k_1-1}) \cdots (p_i^{k_i} - p_i^{k_i-1})\right](p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1}-1})$$

$\Rightarrow$ $\phi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_i^{k_{i+1}} - p_i^{k_{i+1}-1})$

$$= p_1^{k_1} p_2^{k_2} \cdots p_i^{k_{i+1}} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_i}\right)$$

$$= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_i}\right)$$

Example Calculate $\phi(360)$

Sol $360 = 2^3 \cdot 3^2 \cdot 5$

$$\therefore \phi(360) = 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$

$$= 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 96$$

Thm 4 For $n>2$ $\phi(n)$ is even

Pf Firstly let us assume that $n=2^k \quad k\geq 2$

$$\therefore \phi(n)=\phi(2^k)=2^k\left(1-\frac{1}{2}\right)=2^{k-1} \leftarrow \text{even}$$

If n is not a power of 2 then it is divisible by and odd prime say p. Hence we may write

$$n=p^k m \qquad k\geq 1 \qquad \gcd(p^k, m)=1$$

$$\Rightarrow \phi(n)=\phi(p^k)\phi(m)$$

$$=\left(p^k-p^{k-1}\right)\phi(m)$$

$$=p^{k-1}(p-1)\phi(m)$$

$\because$ p is odd. Therefore $p-1$ is even

Hence $\phi(n)$ is even.